UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

MARIA ANGELA ALLIAUD, RODRIGO ARMANDO EMBEITA, JUAN JOSE ESQUIVEL, ANDRES SANCHEZ IBARRA, IGNACIO ROQUE LUCERO, individually and on behalf of all others similarly situated, **Plaintiffs,** **-against-** **PAYONEER, INC.,** **Defendant.**	**Civil Action No.: 1:24-cv-5378** **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Maria Angela Alliaud, Rodrigo Armando Embeita, Juan Jose Esquivel, Andres Sanchez Ibarra and Ignacio Roque Lucero (collectively "Plaintiffs"), individually and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to them and on information and belief as to all other matters, by and through undersigned counsel, hereby bring this Class Action Complaint against defendant Payoneer, Inc. ("Defendant" or "Payoneer").

I. NATURE OF THE ACTION

1. This is a class action lawsuit brought by Plaintiffs against Payoneer for failing to protect their funds and personal information. Payoneer is a financial services company that is wholly owned by Payoneer Global Inc., a publicly traded company holding approximately $5.5 billion in customer funds. Payoneer allows payments in "190+ countries and territories" and handles 70 different currencies and offers itself as a "local bank account to get paid on Amazon or by a client." Promising them that their "local receiving accounts act just like local bank."

2. Plaintiffs are foreign nationals specifically targeted by Payoneer who relied on representations when they signed up for Payoneer's services to protect their life savings by placing

them on a purportedly "safe" and "trusted" American financial platform. Payoneer misrepresented its security measures and failed to safeguard users' accounts ("Accounts") from unauthorized access, resulting in significant financial losses for many of its customers when criminals misappropriated their accounts.

3. Plaintiffs and other Payoneer customers pay Payoneer a fee for each transaction they make on its platform. They also receive Mastercard debit cards consistent with what customers would expect from any bank to access their funds held at Payoneer. When customers use the debit cards to withdraw money from ATMs, they pay another fee to Payoneer. Payoneer also offers eligible customers the ability to receive a Capital Advance of funds.

4. Payoneer required customers to use two-factor authenticated ("2FA") protection for its Accounts, whereby a newly generated SMS OTP verification code ("Code") would be entered each time a new funds transfer destination address was added, and then again when money would be wired.

5. Payoneer is aware of the security risks of its platform to its end users (in fact disclaiming them to its shareholders in its holding company's public filings) yet fails to adequately warn these users that their money could be stolen through unauthorized access to their Accounts – access that is easily obtained due to Payoneer's failure to prevent it.

6. Despite Payoneer's representations and purported security features, over the course of only a few days between January 12, 2024 and January 15, 2024, and often after only a few minutes, over 100 Payoneer customers in Argentina, including Plaintiffs, received unsolicited SMS messages with Codes from Payoneer requesting that they change their passwords; notifications that their passwords had been changed without their knowledge and authorization; and notifications that payments had been made from their Accounts to other Payoneer Accounts.

In none of these cases did Payoneer's customers request these password changes or payment transfers. As a result, Plaintiffs and other Payoneer customers suddenly lost access to their Accounts, and by the time they realized this and were able to re-set their passwords, they learned that their Accounts had been emptied of funds ranging from $5,000 to over $60,000.

7. Many Payoneer customers, including Plaintiffs, received an SMS text message right before the fraud was perpetrated, requesting approval of a password reset on Payoneer, which they did not grant. Many, including Plaintiffs, did not click on fraudulent website URLs that they received via SMS messages. And many, including Plaintiffs, did not see the SMS messages until after the heist had been completed since it occurred in the very early morning hours before they were awake.

8. Immediately after the hack, Plaintiffs and other customers contacted Payoneer about the problem and to try to recover their funds.

9. In some cases, Payoneer's customer service was not open yet and was therefore unavailable to block the customers' Accounts in order to prevent further losses and recover their money from the Accounts to which the funds had been fraudulently transferred.

10. In many other cases, despite the gravity of the rapidly evolving situation, Payoneer provided nothing more than canned "form" responses that revealed its manifestly inadequate investigation of customers' complaints. Some of these responses from Payoneer included false reassurances that, despite the acknowledgment of suspicious logins to their accounts, their funds had ***not*** been accessed, even though the funds had already been stolen.

11. Apparently recognizing that its security systems had been breached, Payoneer asked its customers to henceforth communicate with it only via alternative email accounts instead of through SMS and their current email accounts.

12. Worse, Payoneer represented that the stolen funds had been secured and would be returned to customers. However, soon enough Payoneer's solution changed and after a purported investigation it decided to deny its customers' claims and not return all the funds that had been stolen from them. In some cases, without explanation, Payoneer provided an arbitrarily derived percentage of 35% to some customers of their stolen funds, while other customers received absolutely nothing.

13. Payoneer also failed upon notification of the fraud to immediately block its Accounts identified as fraudulent that received unauthorized payments thereby enabling those Accounts to steal other customers' funds.

14. Although some - including Payoneer - have speculated that its customers were subject to phishing attacks and that customers' mobile content was compromised, the fraudsters should not have had access to later Codes required for the transactions.

15. Furthermore, Payoneer's security oversight failed to identify its own users as the hackers, who were accessing other customers' Accounts and provided no means for customers to block their Accounts, cancel transactions or limit transaction amounts and customers' emails.

16. Payoneer publicly stated that its platform was not compromised, and it takes fraud prevention seriously. However, after the attack, it admitted that it was able to switch reset-password flow to contain further fraud. It also disabled password authentication from SMS messages only and instead now requires a password through email and its app if signing in through a computer. Payoneer also now detects new IP addresses and devices that try to access its Accounts and asks customers to verify that the person trying to access the Account is in fact them. These security measures are all customary and reasonable for financial institutions and may have prevented the theft of Payoneer customers' Accounts.

17. This is not the first time that Payoneer failed to identify illicit transactions on its platform. As recently as a few months ago in November 2023, federal and state regulators investigated and financially penalized Payoneer for violating sanctions orders imposed by the Office of Foreign Asset Control that forbids payments to certain countries - like Russia - and individuals – like terrorist and traffickers deemed to be a threat to national security, foreign policy or the economy of the United States. According to regulators, Payoneer's inadequate sanctions screening program, which included insufficient algorithms and oversight failures, were found to be symptomatic of "unsafe and unsound business conduct" under New York law resulting in thousands of violative transactions. Unfortunately, the incident in January 2024 in Argentina indicates that Payoneer has continued to fail to implement effective oversight of its Accounts to identify and stop criminals and protect its customers' Accounts.

18. Similarly, here, Payoneer's faulty security measures including its reliance on SMS-based 2FA and only requiring a SMS code for password recovery made its customers' funds vulnerable to theft. Payoneer did not have in place a means to detect and authenticate if an individual using an unfamiliar IP address to access Accounts was in fact the customer of those Accounts – basic measures used by email servers and banks, among others. Payoneer also failed to screen its own users, who were fraudsters that stole other Payoneer customers' funds.

19. Not only did Payoneer cause Plaintiffs and Class members to lose money ("Funds") and allow cybercriminals to access customers' personal and financial information ("Personal Information"), Payoneer's failures continue to put them at serious, immediate, and ongoing risk and, additionally, caused costs and expenses to them attributable to responding to, identifying, and correcting damages that were reasonably foreseeable as a result of Payoneer's willful and negligent conduct. Furthermore, the fraudsters remain in possession of Plaintiffs' and the Class members'

Personal Information and can sell it to various cyber criminals, who will continue to buy and use it in order to exploit and injure Plaintiffs and Class members around the world.

20. The fraud was caused and enabled by Payoneer's knowing violation of its obligations to abide by best practices and industry standards concerning the security of payment systems. Payoneer failed to comply with security standards and allowed its customers' Funds and Personal Information to be stolen by cutting corners on security measures that could have prevented or mitigated the hack that occurred and failed to adequately investigate and improperly denied Plaintiffs' claims.

II. JURISDICTION AND VENUE

21. The Court has jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2) ("CAFA") because (a) there are 100 or more Class members, (b) at least one Class member is a foreign citizen that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

22. Although Defendant is a Delaware corporation, this Court has personal jurisdiction over Defendant because it is headquartered in New York, it transacted business in this District, and because a substantial portion of the affected interstate trade and commerce described herein was carried out in this District. Payoneer is licensed by the New York Department of Financial Services to operate a money transmission business in New York State.

23. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred.

III. PARTIES

24. Plaintiff Maria Angela Alliaud ("Alliaud") resides in Buenos Aires, Argentina, and is a citizen of Argentina. She decided to sign up for Payoneer in 2018, and began using it in 2020

in order to have a U.S. dollar account to keep her funds safe and avoid the extreme fluctuations and high inflation in Argentina's economy. On January 11, 12 and January 13, 2024, Alliaud received several unsolicited SMS messages and Codes from Payoneer on her phone. While her phone was in airplane mode on January 13, 2024 at 7:16 a.m.[1] – which she viewed 20 minutes later when she was no longer in airplane mode, she received a message through the Payoneer app stating that a transfer of €18,930.00 or about $20,302.54 (despite only transacting in U.S. dollars previously) was successful, and she also received several Payoneer emails stating that her password had been changed and notifying her of a payment of €18,930.00 made to wy068329@163.com (an unknown Account that she did not authorize). After regaining access to her account by resetting the password a couple minutes later, she saw that her Account had been emptied and that Payoneer provided no means for her to cancel the fraudulent transaction. Within five minutes of viewing her emptied Account, she contacted Payoneer and described what had happened providing all the requested information including an alternative email address to use to communicate. On January 15, 2024, she received a form email from Payoneer acknowledging that there had been a suspicious login to her Account, but incorrectly stating that her funds had not been accessed and suggesting that she change her password. Over the next two weeks, Alliaud had additional conversations with Payoneer to seek a return of her stolen funds and each time was assured that she would receive a response within 20 days. However, not until February 6, 2024, did Payoneer email Alliaud indicating that she would receive $7,255.58 - representing about 35% of what had been stolen from her account. Alliaud responded she was not satisfied with this result as it only represented a fraction of her funds stolen from her Account and requested a full return of her funds. In addition to the loss of her funds, Alliaud has spent time inspecting her Account

[1] All times listed are in Argentina's time zone.

and other bank accounts for fraudulent activity. Alliaud has also suffered from the deprivation of the value of her Private Information and the lost benefit of the bargain.

25. Plaintiff Rodrigo Armando Embeita ("Embeita") resides in Buenos Aires, Argentina, and is a citizen of Argentina. He learned about Payoneer from colleagues and friends as a means to obtaining a safe and secure U.S. bank account needed for his payment by American clients for his employment as an information technology engineer. He decided to sign up for Payoneer on March 10, 2013. On January 14, 2024, he received several SMS messages with Codes at 5:54 a.m. When he saw the SMS messages when he awoke at 7:00 a.m. and was unable to log into his Account, Embeita immediately tried calling Payoneer Customer Care, but was unable to reach anyone to help him because it was outside of Payoneer's working hours. He then reset his password, which allowed him to regain access to his Account, and saw that all of his funds of $17,937.26 were transferred out of his Account in two transactions. At 8:27 a.m., he emailed Payoneer about the situation, and at 11:31 a.m., Payoneer changed his username, password and email. Over the next two weeks, through Payoneer WhatsApp customer support, Embeita followed up requesting a return of his funds and was assured multiple times that his funds were secure and would be returned in 20 days. However, on February 7, 2024, Payoneer only returned $6,278.04 representing about 35% of his stolen funds, to which he responded that he wanted a full refund of his funds. In addition to the loss of his funds, Embeita no longer uses Payoneer, but has kept open his Account that he has spent time inspecting and other bank accounts for fraudulent activity. He has also suffered from the deprivation of the value of his Private Information and the lost benefit of the bargain.

26. Plaintiff Juan Jose Esquivel ("Esquivel") resides in Buenos Aires, Argentina, and is a citizen of Argentina. He learned about Payoneer from a friend as a means to obtaining a safe

and secure U.S. bank account needed for his payment for a freelance job for an American company that paid him through a credit card. He decided to sign up for Payoneer in September 2020. On January 12, 2024, Esquivel received SMS messages requesting to change his password, which he did not, and he then received another SMS message stating that it has been changed without his authorization. He immediately changed his password and contacted Payoneer about the incident, while on the phone with Payoneer. Within 15 minutes of the first unsolicited SMS message, he refreshed his screen and saw that all of his funds of $10,998 had been transferred to another Payoneer Account. Payoneer immediately blocked Esquivel's and the recipients' Accounts, and reassured him that he will get back all his funds that have been frozen. On January 16, 2024, Payoneer reactivated his Account. On February 7, 2024, Esquivel received $3,849.30 - representing about 35% of his stolen funds. Later that same day, Payoneer sent an email to him stating that it would refund another $8,849.30, and then subsequently sent another email stating that the first email was a mistake, and it will refund only $3,849.30. On February 9, 2024, Esquivel received $1 to his Account, to which he responded that he wanted a full refund of his funds. In addition to the loss of his funds, Esquivel has spent time inspecting his Account and immediately withdraws any funds received and monitors his other bank accounts for fraudulent activity. He has also suffered from the deprivation of the value of his Private Information and the lost benefit of the bargain.

27. Plaintiff Andres Sanchez Ibarra ("Ibarra") resides in Mendoza, Argentina, and is a citizen of Argentina. He learned about Payoneer from colleagues and friends as a means to obtaining a safe and secure U.S. bank account for his work as a software developer for an American company. He decided to sign up for Payoneer on June 23, 2021. On January 13, 2024, Ibarra first received a SMS message with a Code and with a link if the Code was not requested, which he did

not click. He signed into his Account using biometrics and confirmed that everything looked normal in his Account. On January 15, 2024, he received SMS messages and emails from Payoneer with Codes and indicating that his password had been changed and that a payment of $30,000 was successful. He immediately tried to log into his Account, which he was unable to do, and then reset his password so he could access his Account. However, again within minutes, despite changing his password, he received additional SMS messages and emails from Payoneer with Codes and notification of password changes that he did not make and another notification of a payment of $7,621. He then tried to use his Payoneer card to purchase something and somehow stop the theft, but it was declined. Within another couple minutes, Ibrarra received SMS messages and emails again with Codes and saying that a payment of $9,996 was successful. Within minutes, he received another SMS message with a code and notification of another payment of $9,986.20 that was made. Ibrarra immediately tried calling Payoneer Customer Care, but was told they could not help him because he was inaudible. He changed his password again. However, within another few minutes, he received another SMS message with Codes and notification that his password had been changed and that another payment of $9,800 was made from his Account. By the time he was able to get through to Payoneer again - less than 30 minutes from the time of the first theft (and after changing his password multiple times), Ibarra lost $67,403.20. Payoneer at this point blocked his Account and changed his email to an alternative account. Ibarra provided all of the information requested by Payoneer to authenticate his Account and confirmation that he did not authorize the transactions. Over four hours later, Payoneer sent a form email to Ibarra confirming that suspicious login to his Account had occurred, but incorrectly stating that his funds had not been accessed and that it had reset his password. In follow up calls over the days that followed, Payoneer representatives assured Ibarra that his funds would be returned. On January 19, 2024, Payoneer

stated to Ibarra in a telephone conversation that additional security measures were being implemented so this would not happen again and reassured him that his funds would be returned within 20 days. The following day, Payoneer indicated that it was disabling SMS Codes for password verification, which would be done through email going forward. Subsequent follow up conversations that Ibarra had with Payoneer reiterated that his funds would be returned and were in the Risk Management department and being expedited, but the return of his funds might take longer due to the "massive hack in Argentina." He was also told by Payoneer representatives that the hackers had been located and funds frozen so they would be returned to him. Despite these reassurances, on February 7, 2024, Payoneer sent Ibarra an email stating that it was only able to recover $23,591.12 - representing 35% of his stolen funds to which he replied this partial refund was unacceptable and attempted to elevate his complaint to the executives of Payoneer. However, Payoneer did not respond, and on February 9, 2024, only credited his account an additional $1. In addition to the loss of his funds, Ibarra no longer uses Payoneer, but has kept his Account open and inspects it and his other bank accounts for fraudulent activity. He has also suffered from the deprivation of the value of his Private Information and the lost benefit of the bargain.

28. Plaintiff Ignacio Roque Lucero ("Lucero") resides in Buenos Aires, Argentina, and is a citizen of Argentina. He works as a freelancer for an American travel agency and is paid in U.S. dollars. In order to protect his earnings from Argentina's economic instability, he inquired with one of his colleagues and learned about Payoneer as a method to be paid, store funds, and receive a Mastercard debit card in an American banking platform that would enable him to spend his funds without first converting them to Argentine Pesos. Lucero reviewed Payoneer's website, including its security measures, and was persuaded that Payoneer was secure against fraud. He signed up with Payoneer on May 12, 2022. Over the course of 15 minutes from 8:38 a.m. to 8:53

a.m. on January 13, 2024, Lucero received an email from Payoneer that his password was changed, €24,000 was transferred to Payoneer Account wy068329@163.com and €19,979 was transferred to the same account (or a total of about $47,179.13) - despite only transacting previously in U.S. dollars. Furthermore, this occurred about a half hour after Plaintiff Alliaud informed Payoneer of the fraudulent payments from her Account to this ***same*** Payoneer Account, which should have been blocked at the point of the unauthorized transaction from Lucero's Account to prevent the fraud. A Payoneer representative later admitted to Lucero that the failure to block the fraudulent Account may have been a fault of Payoneer. Minutes later, Lucero attempted to log into his Account and was forced to reset the password and saw that his Account had been emptied. He then immediately contacted Payoneer Customer Care which blocked his Account. In subsequent correspondence with Payoneer, he was assured that his funds would be returned. On January 15, 2024, he received a form email acknowledging the suspicious login to his Account and incorrectly stating that his funds had not been accessed. However, on February 6, 2024, Payoneer transferred to Lucero only $16,856.49 - representing about 35% of his funds that were stolen to which he replied it was unacceptable. In addition to the loss of his funds, Lucero has spent time inspecting his Account for fraudulent activity and trying to payout his funds from there as quickly as possible to prevent further theft of his funds. He has also suffered from the deprivation of the value of his Private Information and the lost benefit of the bargain.

29. Payoneer is a Delaware corporation headquartered in New York, New York. It self-describes itself as a Money Service Business registered with FinCEN and is a licensed money transmitter under the laws of various states in the U.S., and its services and related disclosures are governed by the laws of the State of Delaware in the United States of America. It provides a global digital financial platform to customers across the world particularly in emerging markets

specializing in cross-border transactions for small and medium size businesses and freelancers. It is a subsidiary of public holding company Payoneer Global Inc. (PAYO), a Delaware corporation located in New York, New York. According to its recent Securities and Exchange Commission ("SEC") filing Form 8-K on February 28, 2024, it held $6.4 billion of customer funds as of December 31, 2023, and in 2023, generated 32% revenue growth, over $90 million of net income, and quadrupled adjusted EBITDA to over $200 million.[2]

IV. FACTUAL BACKGROUND

A. Payoneer's Financial Services and Security Representations to Customers

30. Payoneer proclaims to provide a "quick, secure, and reliable" global digital bank account to its customers to pay, use and receive funds. It accepts all currencies and consolidates them in one Account for its customers eliminating the need for local banks especially for individuals working for international companies that avoids establishing international bank accounts, expensive wire transfer fees and currency conversions. Instead, Payoneer customers can make payments directly from their Accounts, withdraw locally, or use the Payoneer Mastercard debit card at ATMs, online, and in brick-and-mortar stores. Payoneer even offers Capital Advance to certain of its customers.[3]

31. In contrast to what Payoneer offers, American banks have strict requirements on how and if accounts can be established for non-residents and for businesses located outside the country in order to prevent money laundering and other international criminal activity including losses from fraud. Payoneer advertises itself as a "simpler solution" for individuals and businesses located outside the US to effectively set up a US bank account without the "colossal hassle" of

[2] Payoneer, SEC Form 8-K, Feb. 28, 2024, https://d18rn0p25nwr6d.cloudfront.net/CIK-0001845815/fc621b9d-4721-41ae-a024-dc2e0446e778.pdf (last visited Apr. 3, 2024).

[3] Payoneer, Freelancers, https://www.payoneer.com/freelancer/ (last visited Apr. 16, 2024).

doing so:

	US Bank Account	Payoneer
Application	In person, in the U.S.	Online
Financial Information	US business registration US W-8BEN US business address US tax ID (EIN) Business documentation	Name, contact info, local bank account information*
Documentation needed at registration	Your interaction with our websites. Other information collected through Cookies and other tracking technologies as listed above and as described in our "Cookies Policy"	From you directly and our third party analytic tools and cookies usage (See our "Cookies Policy" for more information).
Fees	Monthly account fee Wire transfer fees	Per transaction
Setup time	3-10 days	Same day

> Your Payoneer account, for example, includes local receiving numbers – just like bank account numbers – in the US, EU, UK and Japan. You can get paid into these account numbers ***just as easily as if you had opened a bank account in those countries*** by with far less hassle. When you receive those payments, you can then withdraw the funds to your local bank account in your own currency or use them in a host of other ways. This way, you can receive global payments just as easily as you would locally, saving you and your clients the time, effort and cost of a global bank transfer.
> For marketplace sellers, such as those who sell on Amazon.com, your local US receiving account is a very simple and ***secure way to receive your payments***.
> Payoneer provides a fast payment path between buyer and seller, across borders and currencies, with relatively simple setup, entirely online.
> Both buyers and sellers can register themselves on the service quickly in some 200 countries worldwide, and be exchanging in a matter of days — for far less than the wire transfer fees charged by conventional banks.[4]

32. Payoneer - like a US bank - states that the "core obligation at Payoneer is to ***protect***

[4] Payoneer, How to Open a US Bank Account, https://www.payoneer.com/resources/online-banking/how-to-open-us-bank-account/ (last visited Apr. 4, 2024) (emphasis added).

your funds and prevent money laundering. . . . When partnering with us, you can be assured that all your payee disbursements are made through a ***fully compliant, secure and tightly audited payments platform*** that is recognized by financial regulators all around the world."[5]

33. Payoneer admits that when customers are deciding what to use to "move their money around," "trust" of the company that holds their funds is important. To evidence that Payoneer can be trusted by customers, it touts that its "track record go[es] back to 2005, is publicly listed (Nasdaq: PAYO) and trusted by the biggest brands in tech, banking, and business."[6]

B. Payoneer's Terms and Conditions Regarding its Services

34. Although Plaintiffs entered agreements with Payoneer to use its services before January 2024, however, Payoneer routinely updates the agreement's terms and conditions ("T&C") that become immediately effective upon notice according to Section 2.2. Upon information and belief, the T&C that were in place in January 2024 were first noticed in November 2023.

35. Section 1 of the T&C provides that Payoneer's services are governed by the laws of the State of Delaware.

36. Section 3 describes that the customer appoints Payoneer as its agent to accept payments on its behalf and to make payments. Although Section 3.5 disclaims that it is a bank account (unlike its public advertising to lure in customers to sign up for Payoneer), it states that:

> However, we strictly adhere to applicable requirements which are designed to ensure the safety and liquidity of funds held on behalf of customers including segregation of customer funds and having secured surety bonds to provide additional security for your funds.

[5] Payoneer, Multi-Jurisdictional Licenses, https://www.payoneer.com/legal/payoneers-multi-jurisdictional-licenses/ (last visited Apr. 4, 2024).

[6] Payoneer, About, https://www.payoneer.com/about/ (last visited Apr. 23, 2024).

37. Section 4.5 indicates that some transactions may be reversed and Section 4.7 (and 5.10) indicates that within Payoneer's sole discretion, it may reject or limit transactions.

38. Section 10.7, as well as others, provide that requests for withdrawal and transfer of funds may be denied and additional information to confirm your identity, address, bank account and other information regarding the source of funds may be required.

39. Section 11 details that you can make a payment from your Payoneer balance to another user's Payoneer balance if the user is a registered user of Payoneer or to that person's bank account if it was pre-approved by Payoneer.

40. Section 16 details the registration to use Payoneer subject to Payoneer's Know Your Customer process and approval policies.

41. Section 17 relates to maintenance of Payoneer Accounts. Section 17.4 states that:

In order to file a claim for an unauthorized or incorrectly executed transaction, you must immediately notify us after becoming aware of the unauthorized or incorrect transaction and in any event no later than sixty(60) days after the debit date of the transaction, and with respect to any Payoneer Card transaction, you must follow the instructions provided by the Issuer pursuant to such Issuer's terms and conditions.

42. Section 18 pertains to keeping Payoneer Accounts safe. Section 18.1 states that your Account is safeguarded by a password that you must keep safe and change regularly and not disclose to any third party except on Payoneer's website. Section 18.2 states that Payoneer may require you to verify your identity when signing-into your Payoneer Account and from time to time when using certain of the Payoneer Services by sending a verification code to your mobile phone via SMS ("Two Step Verification").

43. Section 18.3 requires that you must immediately change your password and contact

Payoneer Customer Care if you noticed any suspicious activity regarding your Account. This section also denotes that "[a]ny delay in or failure to notify us may not only affect the security of your Payoneer Account but may result in you being liable for any losses as a result.

44. Section 18.4 states that Payoneer may "suspend your Account or otherwise restrict its functionality (including access to funds), in its sole discretion, on grounds relating to the security of the Payoneer Account or any of its security features or if we suspect that an unauthorized or fraudulent use of your Payoneer Account has occurred or that any of its security features have been compromised."

45. Section 18.5 requires ensuring that your email and mobile phone are kept secure and only accessed by you and that you should notify Payoneer of any compromise. Section 18.6 indicates that any login details should not be stored. Section 18.7 indicates that other Payoneer products or services may have additional security requirements as specified in their applicable terms and conditions. Section 18.8 requires that only the individual named in Payoneer records is authorized to use the Payoneer Services and if you allow another person to have access (except as provided in 18.9 and 19), Payoneer will treat this as if you have authorized such use, and you will be liable for all transactions and fees incurred by such use.

46. Section 21 relates to prohibited uses of Payoneer including fraud. Section 21.8 states that if it is determined that a prohibited use occurs the transaction may be reversed, Account suspended or terminated, reported to law enforcement and damages may be claimed.

47. Section 23 details Payoneer's privacy policy and that it retains personal information about customers and may disclose them if necessary.

48. Section 24.3 states:

In case of a (i) bona fide unauthorized payment or (ii) payment that was incorrectly

executed due to an error by us, ***we shall at your request promptly refund the payment amount including all fees deducted therefrom***. This shall not apply:

- where the unauthorized payment arises from your failure to keep the personalized security features of your Payoneer Account safe in accordance with the provisions of Keeping Your Payoneer Account Safe above;
- if you fail to notify us immediately of any loss of your password or other event that could reasonably be expected to have compromised the security of your Payoneer Account after you have gained knowledge of such event in which case you shall remain liable for losses incurred up to your notification to us;
- in case the transaction was unauthorized but you have compromised the security of your Payoneer Account with intent or gross negligence; or
- if you fail to dispute and bring the unauthorized or incorrectly executed transaction to our attention within sixty (60) days from the date of the transaction.

49. Section 24.4 Payoneer recommends checking transactions in your Account history regularly and frequently. It states that "to the extent the security of the email account used to register for the Payoneer Services has been compromised, Payoneer shall not be liable for any funds lost, or any unauthorized payments made, as a result of such compromise."

50. Section 24.5 states that "[i]n case of any incorrect or misdirected payment made by you, we shall take reasonable measures to assist you with tracing and, if reasonably possible, recovering such payments, but we shall not be liable for any payments that cannot be recovered.

51. Section 24.6 states that Payoneer is not liable for any abnormal or unforeseen beyond Payoneer or third parties' control disruption or impairment of our service or for disruptions or impairments of intermediary services on which we rely for the performance of our obligations.

52. Section 24.8 provides that "[n]othing in these Terms and Conditions shall operate to exclude liability for gross negligence, fraud or fraudulent misrepresentation or for any statutory liability that cannot be excluded or amended by agreement between the parties."

53. Despite Section 24.8's acknowledgment that the agreement cannot disclaim liability, Sections 24.12 and 24.13 attempt to do so and to limit any damages to fees paid to Payoneer and permitting one year to bring a claim.

54. Section 25 provides for termination of Accounts including for false information and fraud.

55. Section 26.8 provides that although most communications will be via email and through Payoneer's website, it may contact customers via letter, telephone, SMS or mobile phone, and require communication via SMS in order to authenticate payments, help you reset your password, authenticate other activity or for other security purposes.

56. Section 27 details the complaint process. 27.1 states that complaints should be made by contacting Payoneer Customer Care which may be followed up by an acknowledgement and request for additional information. Section 27.2 states that Payoneer's "goal is to provide you with a prompt answer or resolution to your complaint where possible. Nothing contained herein, however, constitutes a commitment by Payoneer to resolve your complaint."

C. Payoneer Is Aware of Risks of Fraud on its System, Yet Failed to Protect its Customers

57. In the years preceding Payoneer's announcement of the Argentina Attack, rampant reports of fraud on customers, who use payment platforms have been the subject of Congressional

scrutiny,[7] media reports[8] and lawsuits.[9] Payoneer knew or should have known that its customers' funds were squarely within the crosshairs of hackers.

58. Despite this, it did not adequately warn its customers of the risk of their funds being stolen from its platform. Only identifying on a buried page on its website under "resources," "the most common types of payment fraud in business today" – not standard, periodic pop-up reminders that customers must indicate they have read:

- **Account takeover:** In an account takeover, fraudsters gain ***unauthorized access*** to legitimate accounts by stealing login credentials or using social engineering techniques.
- **Phishing scams**: Phishing scams can involve fake emails, text messages, or phone calls that trick people into giving away sensitive information, such as login credentials or financial details. Fraudsters often pose as reputable organizations, enticing victims to click on malicious links or provide confidential information.
- **Credit card fraud:** Credit card fraud is when fraudsters gain unauthorized access to credit card information and use it to make fraudulent purchases or cash withdrawals. This can involve physical theft of the card, skimming card details, or online hacking of card information.
- **Identity theft**: Identity theft involves the fraudulent use of someone's personal

[7] US Senate Committee on Banking, Housing and Urban Affairs, Brown, Reed, Warren Urge Venmo, Cash App to reimburse victims of Fraud and Scams, Dec. 14, 2023, https://www.banking.senate.gov/newsroom/majority/brown-reed-warren-urge-venmo-cash-app-to-reimburse-victims-of-fraud-and-scams (last visited Apr. 16, 2024).

[8] Forbes, 7 Peer-to-Peer Payment Scams and How to Avoid them, Oct. 25, 2023, https://www.forbes.com/advisor/money-transfer/p2p-scams/ (last visited Apr. 16, 2024).

[9] Vixio, US Banks May Pay for Zelle Fraud As Lawsuits Mount, Jun. 8, 2022, https://www.vixio.com/insights/pc-us-banks-may-pay-zelle-fraud-lawsuits-mount (last visited Apr. 16, 2024).

information, including their name, Social Security number, and/or financial account details, without their consent. Fraudsters use stolen identities to open new accounts, make unauthorized transactions, or commit other forms of financial fraud.

- **Mobile payment fraud**: With the rise of mobile payment apps, ***fraudsters have targeted these platforms for fraudulent activities***. This can include using stolen payment credentials, exploiting vulnerabilities in the app's security, or ***conducting unauthorized transactions***.[10]

59. In the minimal disclosure it did make to its customers, Payoneer suggested that if customers took certain steps including monitoring their transactions, immediately reporting suspicious activity such as unauthorized transactions and implementing security measures - like 2FA – two-factor authentication for transactions and account access (all of which Plaintiffs did), they could prevent this risk:[11]

Preventing payment fraud is a critical aspect of protecting businesses from financial losses and reputational damage. Here are our top recommendations for how to protect yourself from fraud:

- **Use secure payment systems**: Ensure that your payment systems and infrastructure are secure. This includes using encryption technology to protect sensitive data during transmission and storing customer information in a secure manner.
- **Two-factor authentication**: Implement two-factor authentication (2FA) for online transactions and account access. ***2FA adds an extra layer of security by requiring***

[10] Payoneer, Fraud, https://www.payoneer.com/resources/fraud/ (last visited Apr. 16, 2024) (emphasis added).

[11] *Id*.

users to provide additional verification, such as a unique code sent to their mobile device, in addition to their username and password.

- **Employee training and awareness:** Educate your employees about payment fraud risks and prevention measures. Provide training on how to identify and report suspicious activities.
- **Fraud detection systems**: Deploy robust fraud detection systems that can monitor transactions in real-time and detect potentially fraudulent activities. Set up alerts and thresholds to flag potentially fraudulent activities for further investigation.
- **Regular account reconciliation**: Regularly reconcile your financial accounts to ***identify any unauthorized or fraudulent transactions promptly***. Monitor transaction histories, bank statements, and payment processor reports to ensure all transactions are legitimate. Report any discrepancies or suspicious activities to the appropriate authorities.
- **Strong password policies**: Enforce strong password policies for your customers and employees. Encourage the use of complex passwords that include a combination of letters, numbers, and special characters. Regularly prompt users to update their passwords and consider implementing password expiration policies.
- **Vendor due diligence**: Conduct due diligence when selecting and working with third-party vendors, payment processors, and service providers. Ensure they have robust security measures in place to protect your payment data. Review their security policies, certifications, and track record in handling payment transactions securely.[12]

[12] *Id*. (emphasis added).

60. In contrast to lack of disclosure of risks to customers and its own failure to protect its customers' funds and personal information, its parent holding company, Payoneer Global, publicly acknowledges to its shareholders the risks to its business from fraud instigated by its own users:

> ***Failure to effectively deal with bad, fraudulent or fictitious transactions and material internal or external fraud could materially negatively impact our business.***
>
> We have been, and may in the future be, subject to liability for fraudulent transactions, including electronic payments and card transactions or credits initiated by customers. . . . Criminals are using increasingly sophisticated methods to engage in illegal activities such as counterfeiting, ***account takeover and fraud***. It is possible that incidents of fraud could increase in the future. Failure to effectively manage risk and prevent fraud, or otherwise effectively administer our chargeback responsibilities, would increase our chargeback liability, exposure to fines or other liabilities. Increases in chargebacks, fines or other liabilities could have a material adverse effect on our business, results of operations and financial condition. [13]

61. Payoneer Global also acknowledges to its shareholders the risk to its customers of such attacks:

> ***Cyberattacks and security vulnerabilities could result in material harm to our reputation, business, financial condition and results of operations, and unauthorized disclosure, destruction or modification of data, through cybersecurity breaches, computer viruses or otherwise, or disruption of our services, could expose us to liability and/or damage our reputation.***
>
> We are subject to a number of legal requirements, regulations, contractual obligations and industry standards regarding security, data protection and privacy and any failure to comply with these requirements, regulations, obligations or standards could have a material adverse effect on our reputation, business, financial condition and operating results.
>
> In conducting our business, we collect, process, transmit, store, use and share sensitive business information and PII about our customers, financial institution partners, vendors, and other parties. This information may include account access credentials, credit and debit card numbers, bank account numbers, social security numbers, passport/ID numbers, driver's license numbers, names and addresses and other types of sensitive business information or PII, including copies of documents thereof. Some of this information is also

[13] Payoneer, SEC Form 10-K, Feb. 28, 2024 ("10-K"), at page 18 https://d18rn0p25nwr6d.cloudfront.net/CIK-0001845815/643fba91-fd73-4a6e-8754-c3f5df847860.pdf (last visited Apr. 3, 2024) (emphasis added).

collected, processed, stored, used, shared and transmitted by our software and financial institution partners, third-party service providers to whom we outsource certain functions and other vendors. We have certain responsibilities to payment networks and their member financial institutions for any failure, including the failure of our associated third-party service providers, to protect this information. Information security risks for financial and technology companies such as ours have significantly increased in recent years in part because of the proliferation of new technologies, the use of the Internet and telecommunications technologies to conduct financial transactions, and the increased sophistication and activities of organized crime, hackers, terrorists and other external parties. Because of our position in the payments value chain, we believe that we are likely to continue to be a target of such threats and attacks. Additionally, geopolitical events and resulting government activity could also lead to information security threats and attacks by affected jurisdictions and their sympathizers. As artificial intelligence capabilities continue to evolve, they may be used to identify vulnerabilities and craft sophisticated cybersecurity attacks. Vulnerabilities may be introduced from the use of artificial intelligence by us, our customers, vendors and other business partners and third-party providers. If these attempts are successful it could lead to the compromise of sensitive or confidential business information or PII.

In addition, our products, services and customers may themselves be targets of cyberattacks that attempt to sabotage or otherwise disable them, and the defensive and preventative measures we take ultimately may not be able to effectively detect, prevent, or protect against or otherwise mitigate losses from all cyberattacks. Any such breach or attack could compromise our platform, creating system disruptions or slowdowns and exploiting security vulnerabilities of our products and services. Additionally, in case of such breach, the information stored on our platform could be accessed, publicly disclosed, lost, or stolen, which could subject us to substantial liability and cause us material financial harm. These breaches, or any perceived breach, may also result in damage to our reputation, negative publicity, loss of key business relationships and sales, increased costs to remedy any problem (including repairing system damage, increasing security protection costs by deploying additional personnel and modifying or enhancing our protection technologies and investigating and remediating any information security vulnerabilities), regulatory inquiries and investigations, customer complaints and costly litigation and legal expenses, and may therefore adversely impact market acceptance of our products and materially adversely affect our business, financial condition or results of operations.

We have in the past, and may in the future, be the target of malicious third-party attempts to identify and exploit system vulnerabilities, and/or penetrate or bypass our security measures, in order to gain unauthorized access to our platform and systems. If these attempts are successful it could lead to the compromise of sensitive or confidential business information or PII. The systems and procedures we have in place to defend against intrusion and attack and to protect our data may not be sufficient to counter all current and emerging technology threats.

Our computer systems and the computer systems of our third-party service providers and software partners have been, and in the future could be, subject to breaches, and our data

protection measures may not prevent unauthorized access. While we believe the procedures and processes we have implemented to handle an attack are adequate, the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently and are often difficult to detect. In addition, increased remote operations creates an additional risk of attack while decreasing our ability to monitor. Threats to our systems and associated third-party systems can originate from human error, fraud or malice on the part of employees or third-parties, or simply from accidental technological failure. Computer viruses and other malware can be distributed and could infiltrate our systems or those of third-party service providers. In addition, denial of service attacks, phishing scams, social engineering, ransomware theft, cyber-attacks created through or due to use of artificial intelligence or other attacks could be launched against us or our customers for a variety of purposes, including to interfere with our services or create a diversion for other malicious activities. Our defensive measures and training may not prevent unplanned downtime, unauthorized access or unauthorized use of sensitive business data or PII.

While we maintain cyber errors and omissions insurance coverage that covers certain aspects of cyber risks, our insurance coverage may be insufficient to cover all losses. The successful assertion of one or more large claims against us in this regard that exceed our available insurance coverage, or the occurrence of changes in our insurance policies, including premium increases or the imposition of large deductible or coinsurance requirements, could have a material adverse effect on our reputation and our business, financial condition and results of operations. We also cannot ensure that our existing insurance coverage will continue to be available on acceptable terms or will be available in sufficient amounts to cover one or more large claims related to a security incident or breach, or that the insurer will not deny coverage as to any future claim. Further, while we select our third-party service providers carefully, we do not control their actions. Any problems experienced by these third-parties, including those resulting from breakdowns or other disruptions in the services provided by such parties or cyber-attacks and security breaches, could materially adversely affect our ability to service our customers or otherwise conduct our business.

Further, use of technologies based on artificial intelligence by our employees, whether authorized or unauthorized, may increase the risk that PII, our intellectual property and other proprietary information will be unintentionally disclosed, compromised, or that we may infringe on the intellectual property rights of others. We could also be subject to liability for claims relating to misuse of PII, such as unauthorized marketing purposes and violation of consumer protection or data privacy laws. In addition, federal, state and foreign rules and regulations may require us to notify individuals of data security incidents involving certain types of PII or information technology systems. We cannot provide assurance that the contractual requirements related to security and privacy that we impose on our service providers who have access to customer data will be followed or will be adequate to prevent the unauthorized use or disclosure of such data. In addition, we have agreed in certain agreements to take certain protective measures to ensure the confidentiality of customer data. The costs of systems and procedures associated with such protective measures may increase and could adversely affect our ability to compete effectively. Any failure to adequately enforce or provide these protective measures could

> result in liability, protracted and costly litigation, governmental and card network intervention and fines and, with respect to misuse of PII of our customers, lost revenue and reputational harm.
>
> Any type of security breach, attack or misuse of data, whether experienced by us or an associated third-party, could harm our reputation or deter existing or prospective customers from using our services, increase our operating expenses in order to contain and remediate the incident, expose us to unbudgeted or uninsured liability, disrupt our operations (including potential service interruptions), divert management focus away from other priorities, increase our risk of regulatory scrutiny, result in the imposition of penalties and fines under state, federal and foreign laws or by card schemes and adversely affect our regulatory licenses and banking relationships. Further, if we were to be removed from networks' lists of Payment Card Industry Data Security Standard, our existing customers and financial institution partners or other third parties may cease using our services.[14]

D. Payoneer's Checkered History of Inadequate Security Measures

62. Despite its knowledge of these fraud risks to the Company and its customers, Payoneer has a history of failing to enact proper security measures to ensure illegal transactions are not occurring on its platform.

63. When US Treasury documents were leaked in 2020, referred to as "FinCEN Files," some of the suspicious activity reports included Payoneer. Some complaints about Payoneer were related to its prepaid debit cards, which Payoneer customers were shocked to learn were secured by an "offshore" Belize bank and not through Payoneer, which they had signed up with for the service originally, and only came to light when the Belize bank went under and lost the customers' funds. Other reports included over $800 million in suspicious transfers by Payoneer over the six-year period (with the most during 2014-16), saying they "show an unusual pattern of potential deceptions involving far-flung corporate entities, anonymous shell companies, and secretive offshore finance." Another report highlighted a $38 million in Payoneer transactions because the reporting bank was "unable to confirm the commercial purpose of any of these transactions

[14] 10-K at page 22-23.

through independent research." A separate report flagged a $20.6 million in payments Payoneer received from an "online adult video streaming site linked in news reports to human trafficking." Although the reports themselves are not considered proof of wrongdoing, they are used by regulators and law enforcement to investigate potential violations and criminal behavior such as money-laundering.[15]

64. In 2021, the U.S. Treasury Department of Office of Foreign Assets Control ("OFAC") announced that it agreed to a settlement with Payoneer after uncovering 2,220 violations of multiple sanctions programs whereby Payoneer would pay a penalty of nearly $1.4 million. Payoneer only self-reported about 19 of the over 2,000 prohibited payments from February 4, 2013 to February 20, 2018, that were processed for persons located in Crimea region of Ukraine, Iran, Sudan, and Syria and on behalf of sanctioned persons among others.[16]

65. In its investigation, OFAC found that "Payoneer's sanctions compliance program deficiencies at the relevant times—including with respect to screening, testing, auditing, and transaction review procedures—enabled persons in these jurisdictions and regions and on the SDN (sanctions) List to engage in approximately $793,950.70 worth of transactions." Specifically, OFAC found that weak algorithms and screening failed to detect those on the sanctions list; during backlog periods, flagged and pending payments were released without review and it failed to monitor IP addresses or addresses in flagged locations.[17]

---

[15] NBC News, Secret Documents Reveal Potential Dark Side of Prepaid Debit Cards, Sept. 22, 2020, https://www.nbcnews.com/business/consumer/secret-documents-reveal-potential-dark-side-prepaid-debit-cards-n1240332 (last visited Apr. 23, 2024).

[16] OFAC, OFAC Enters Into $1,385,901.40 Settlement with Payoneer Inc. for Apparent Violations of Multiple Sanctions Program, July 23, 2021, https://ofac.treasury.gov/media/911571/download?inline (last visited Apr. 23, 2024).

[17] *Id*.

66. In determining the penalty, OFAC found the following aggravating factors:

1) Payoneer ***failed to exercise a minimal degree of caution or care*** for its sanctions compliance obligations when it allowed persons on the SDN List and persons in sanctioned locations to open accounts and transact as a result of deficient sanctions compliance processes that persisted for a number of years;

2) Payoneer had reason to know the location of the users it subsequently identified as located in jurisdictions and regions subject to sanctions ***based on common indicators of location within its possession, including billing, shipping, or IP addresses, or copies of identification issued in jurisdictions and regions subject to sanctions***; and

3) The Apparent Violations caused harm to six different sanctions programs.[18]

67. Payoneer declared, as part of its improvement to its security, to OFAC that it would be "enabling the screening of names, shipping and billing addresses, and IP information associated with account holders" among other measures.[19]

68. On November 2, 2023, the New York State Department of Financial Services, announced it had entered an additional Consent Order involving Payoneer's processing of payments in violations of the sanctions programs that also violated New York law where it is licensed and operates its business. Payoneer agreed to pay $1.25 million to the Department as a penalty and as its promise to OFAC would implement enhanced oversight to ensure that it did not violate sanctions orders.[20]

E. Payoneer's Failed Security Measures Enabled the Hack of Payoneer Customers'

[18] *Id.*

[19] *Id.*

[20] New York State Department of Financial Services, In the matter of Payoneer Inc., Consent Order, November 2, 2023, https://www.dfs.ny.gov/system/files/documents/2023/11/ea20231102_co_payoneer.pdf (last visited Apr. 23, 2024).

Accounts in Argentina

69. Over the course of only a few days in mid-January 2024, fraudsters accessed Payoneer customers' Accounts in Argentina - that had been safeguarded as required and not compromised (including their emails) by any fault of Payoneer customers themselves - and without those customers' knowledge and authorization, transferred their funds to other Payoneer Accounts (the "Hack"). Many lost years of their employment earnings.[21]

70. During the Hack, many Payoneer customers received unsolicited SMS messages from Payoneer with codes to verify their Accounts and change their passwords on the date their Accounts were emptied. Affected users reported the Hack on social media with hundreds of posts.[22]

71. Consistent with the experience of other victims of the Hack, Plaintiffs received unsolicited SMS messages notifying them that their passwords had been changed without their authorization and payments that they did not authorize were made. When they changed their passwords and were able to regain access to their Accounts, they saw that their funds had been stolen by other Payoneer Accounts.

72. Furthermore, Plaintiff Alliaud and Lucero's Accounts were drained of funds in Euros instead of US dollars, which they had only previously used. Their funds were also transferred to the same unknown Payoneer Account even though Plaintiff Alliaud alerted Payoneer to the Hack a half hour before Lucero's funds were stolen.

73. Plaintiff Alliaud lost $20,302.54. Plaintiff Embeita lost $17,937.26. Plaintiff

[21] Buenos Aires Herald, Dozens of Argentine Payoneer users report hackings and emptied accounts, Jan. 20, 2024, https://buenosairesherald.com/society/dozens-of-argentine-payoneer-users-report-hackings-and-emptied-accounts (last visited Apr. 24, 2024).

[22] *Id.*

Esquivel lost $10,998. Plaintiff Ibarra lost $67,403.20. Plaintiff Lucero lost $47,179.13. Plaintiffs and other customers lost their funds within minutes of receiving the unsolicited SMS messages from Payoneer and had no means to block their Accounts or cancel the transactions.

74. Another Payoneer customer reported that he noticed the Hack when he received notifications that purchases were made with his Payoneer debit card in supermarkets in the United States while he was in Mar del Plata, Argentina. He lost close to $1,000.[23]

75. A computer security expert and journalist, Julio López, opined on social media that the breach most likely came through hackers intercepting SMS codes that Payoneer sent to its customers to verify their identities through a cellphone service provider. Lopez also indicated that the hackers likely used this same maneuver to create a phishing website from which they took the Payoneer customers' email addresses. However, other victims of the Hack - including Plaintiffs - did not click on any links that they received or fall for any phishing websites. Movistar, the cellphone service provider, has denied any responsibility related to the Hack.[24]

76. When reporters contacted Payoneer about the Hack, it did not respond to requests for comment about what victims are supposed to do now that their funds are gone, and it is still unclear how the hackers were able to bypass several layers of security to conduct the attacks.[25]

77. Security experts have noted that SMS-based two-factor authentication that Payoneer utilized is easy to hack and bypass and many companies no longer use it for that reason

[23] *Id.*

[24] *Id.*

[25] The Record, Financial Platform Payoneer Blames Account Hacks on Phishing Campaign, Jan. 19, 2024 https://therecord.media/financial-platform-payoneer-account-hacks-phishing (last visited Apr. 24, 2024).

including Google and Microsoft that moved toward more phishing-resistant forms of MFA.[26]

78. Another report pointed out that if the Hack of the Payoneer SMS codes was orchestrated through access to the cellphone carrier, it did not include emails that should have been required to access the Accounts. Another theory is that the SMS provider that Payoneer uses to deliver its Codes was breached, allowing the threat actors to access codes sent by Payoneer.[27]

79. Although Payoneer indicated it believed the Hack was a result of phishing blaming its customers for providing their credentials to the fraudsters, many – including Plaintiffs - did not click on phishing links. Payoneer customers instead accuse Payoneer of attempting to deflect responsibility and failing to acknowledge a potential error or vulnerability within the platform.[28]

80. Following the Hack, it was reported that Payoneer requires a new SMS OTP code to be entered when you add a new destination address and then again when you wire money. If this was a phishing attack stealing OTP codes for the password reset, the threat actors should not have had access to later OTP codes required for these transactions.[29]

81. Although the precise mechanism of the Hack remains unclear, news reports all identify a significant weakness in Payoneer's system as its reliance on SMS-based 2FA. This security issue is compounded by the fact that Payoneer's password recovery process only required an SMS code. As a result until further information about the Hack comes to light, one report advised Payoneer users in Argentina to withdraw funds from their Accounts or disable SMS-based

[26] *Id*.

[27] Bleeping Computer, Payoneer accounts in Argentina hacked in 2FA bypass attacks, Jan. 19, 2024, https://www.bleepingcomputer.com/news/security/payoneer-accounts-in-argentina-hacked-in-2fa-bypass-attacks/ (last visited Apr. 24, 2024).

[28] *Id*.

[29] *Id*.

2FA and reset their Account password.[30]

F. Adding Insult to Injury Payoneer Inadequately Investigates Customers' Claims and Improperly Denies Them

82. Immediately after finding out that their funds had been stolen through unauthorized access to their Accounts in the Hack, customers - including Plaintiffs - contacted Payoneer Customer Care for help and reported the transactions to other Payoneer Accounts (improperly vetted by Payoneer) that occurred were not authorized in compliance with T&C sections 24.3 and 27.1. They immediately changed their passwords and many had their Accounts blocked to stop any further theft. They agreed to provide alternative emails to communicate with Payoneer and all identifying information requested by Payoneer to confirm who they were and that they did not authorize the transactions.

83. While T&C section 27.2 requires that Payoneer provide a prompt answer and resolution to customer complaints, Payoneer representatives focused instead on reassuring their customers that Payoneer was safe to use and their funds were secure and not to withdraw them or stop using Payoneer. Payoneer went so far as to send "form" emails soon after the Hack to its customers – including to Plaintiffs - recognizing that there were suspicious logins to their Accounts, but incorrectly stating that their funds were ***not*** accessed. Later, when Plaintiffs followed up on the status of the return of their funds, they were again falsely reassured that their funds would be returned. Some representatives stated that it would take 20 days before their funds would be returned, and one stated to Plaintiff Lucero it might take longer due to the "massive attack in Argentina."

84. As a result, Plaintiffs waited weeks after the Hack occurred to find out that Payoneer was only returning to them 35% of their funds stolen from their accounts. On January

[30] *Id.*

23, 2024, Payoneer posted a statement on its website about the fraud that occurred in Argentina. It downplayed the incident describing it as a phishing scam and blamed its own customers for the thefts to their Accounts:

> During the weekend of January 13 and 14, a ***small number of Payoneer customers*** in Argentina were victims of an organized fraud scheme that led to certain customers' funds being stolen. Payoneer's internal investigation into ***recent phishing scams*** impacting some customers in Argentina is ongoing, and we are ***working non-stop to help them recover funds where possible and to identify and help stop the criminal actors behind these scams***. The situation was quickly contained, affecting approximately 100 customers.
>
> At ***no point were Payoneer's enterprise systems or platforms compromised***. Rather, the fraudsters were able to access customer accounts through ***external vulnerabilities***. In some cases, fraudsters lured customers to click on links to phishing sites and provide their account credentials. In some other cases, customers had their mobile lines or SMS content compromised, as recently happened in some countries in the region, where local mobile carriers identified this type of loophole on their networks. ***Payoneer took swift action to contain the fraud attempts and prevent spreading, switching the reset-password flow to mitigate further phishing attempts***, and there have been no further cases reported since January 17th.
>
> Although this incident did not involve any direct compromise of Payoneer's platform, ***we are looking at ways to support customers who have been defrauded by the criminals***. As we are working directly with affected customers, we do not anticipate having further public updates on this matter. We take fraud prevention very seriously and continue to work closely with regulators, mobile carriers, and law enforcement agencies to help combat financial crime. We encourage customers to remain vigilant against fraudsters and to educate themselves on how to keep their accounts safe and protect their confidential information.[31]

85. Despite Payoneer's statements that their funds had not been accessed and would be returned and acknowledging suspicious logins to their Accounts and the Hack, Payoneer conducted inadequate investigations to confirm that unauthorized transactions occurred and improperly denied customers' claims for a full return of their funds.

86. In violation of T&C section 24.3, Payoneer failed upon Plaintiffs' request to

[31] Payoneer, Update on Recent Phishing Activity, Jan. 23, 2024 https://blog.payoneer.com/news/an-update-on-recent-phishing-activity/ (last visited Apr. 4, 2018) (emphasis added).

promptly refund the unauthorized payment amounts including any fees. Instead, Payoneer returned arbitrary amounts representing about 35% of stolen funds to Plaintiffs. However, Payoneer representatives indicated that some customers received all of their stolen funds back that were recovered. Upon information and belief, some Payoneer customers did not receive a return of any of their stolen funds.

87. Furthermore, despite deflecting blame for the Hack, it is widely acknowledged that Payoneer's reliance on 2FA SMS codes created vulnerability to fraudsters, who accessed Payoneer's Accounts. It also failed to block a fraudster's Account identified by Plaintiff Alliaud immediately, which would have prevented the subsequent theft of funds by that same fraudster's Account from Plaintiff Lucero's Account. Payoneer does not provide a way for customers to cancel or stop a transaction or block access to their Account, which could have stemmed the Hack that took place through multiple transactions like Plaintiff Ibarra experienced. Based on the large amounts stolen, Payoneer should have detected the Hack and suspended transactions to protect its customers' funds particularly if the users' domains and IP addresses were inconsistent with those of its customers and unauthorized payments were sent to the same Payoneer Accounts. Instead, Payoneer's failed security, ignoring of red flags and failure to exercise reasonable and industry expected oversight allowed fraudsters to steal tens of thousands of dollars from its customers including Plaintiffs through no fault of their own.

88. Even though Payoneer claimed that its system was not compromised or vulnerable, Payoneer admitted to switching the password reset flow to email from SMS only. It now requires a password or biometric sign in through the app even if you sign in with a computer. Payoneer also now requires a code received through email if a new device or IP address is detected for a customers' Account and customers can approve or deny any new logins (reminiscent of the

monitoring of IP addresses Payoneer promised to do in its settlement with OFAC relating to the transactions in violation of sanctions programs). All of these changes are standard bear in the technology and banking industries and should have been in place in the first place at Payoneer to protect customers' Accounts.

89. Unfortunately, Payoneer's treatment of customers' Funds and their Private Information entrusted to it by its customers fell far short of satisfying its legal duties and obligations. Payoneer failed to ensure that access to its payment system was reasonably safeguarded, failed to acknowledge and act upon industry warnings, and failed to use proper security systems to detect and deter the Hack that occurred. Instead, it allowed thieves to access its customers' Accounts and Personal Information including that of Plaintiffs to steal its customers' funds through other Payoneer Accounts.

G. Payoneer Failed to Meet Industry Standards for Security of its Customers Accounts

90. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses, highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[32]

91. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which establishes guidelines for fundamental data security principles and practices for business.[33] The guidelines note businesses should protect the personal customer

[32] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited April 24, 2024).

[33] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited April 24, 2024).

information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

92. The FTC recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; ***use industry-tested methods for security***; ***monitor for suspicious activity on the network***; and verify that third-party service providers have implemented reasonable security measures.[34]

93. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

94. In this case, Payoneer was at all times fully aware of its obligation to protect its customers' Funds and Private Information because it is a payment platform. Payoneer was also aware of the significant repercussions if it failed to do so because it would lose the trust of its customers and their business if they believed their Funds could be stolen.

[34] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited April 24, 2024).

95. As a result of Payoneer's failure to adhere to industry and government standards for the security of its payment platform, Funds and Private Information of Payoneer customers, including Plaintiffs, was compromised.

H. Hacks of Accounts with Personal Information Can Further Lead to Identity Theft

96. According the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014. Among identity theft victims, existing bank or credit accounts were the most common types of misused information.[35]

97. Private Information—which includes Plaintiffs' and Class members' names, address, contact information combined with their bank account information and in some cases debit card information accessed in the Hack—is a valuable commodity to identity thieves. Plaintiffs' and Class members' personal information is being sold and traded by cyber criminals on the dark web. Criminals often trade the information on the dark web for a number of years.

98. Private information is broader in scope than directly identifiable information. As technology advances, computer programs become increasingly able to scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible.

I. Damages Sustained by Plaintiffs and Class Members

99. As a result of Payoneer's inadequate, non-industry standard security measures to safeguard its Accounts, Plaintiff Alliaud lost $20,302.54, Plaintiff Embeita lost $17,937.26, Plaintiff Esquivel lost $10,998, Plaintiff Ibarra lost $67,403.20, and Plaintiff Lucero lost $47,179.13

[35] *See Victims of Identity Theft, 2014*, DOJ, at 1 (2015), available at https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited April 24, 2024).

as well as cybercriminals' accessing their Personal Information which could lead to further damage to them.

100. Furthermore, a portion of the services purchased from Payoneer by Plaintiffs and the other Class members necessarily included compliance with industry-standard measures with respect to the collection and safeguarding of their Accounts and Private Information. The cost to Payoneer of collecting and safeguarding Accounts and Private Information is built into the price of all of its services. Because Plaintiffs and the other Class members were denied security and privacy protections that they paid for and were entitled to receive, Plaintiffs and the other Class members incurred actual monetary damages not only in the loss of their funds, but also in overpaying their fees to Payoneer.

101. Plaintiffs and the other members of the Class have suffered additional injury and damages, including, but not limited to: (i) an increased risk of identity theft and identity fraud; (ii) improper disclosure of their Private Information, which is now in the hands of criminals; (iii) the value of their time spent mitigating the increased risk of identity theft and identity fraud; (iv) deprivation of the value of their Private Information, for which there is a well-established national and international market—for which they are entitled to compensation.

102. Plaintiffs and the other Class members suffered additional damages based on the opportunity cost and value of time that Plaintiffs and the other Class members have been forced to expend to monitor their financial accounts as a result of the Hack.

103. Acknowledging the damage to Plaintiffs and Class members, Payoneer instructs its customers to take certain cautionary steps of diligently reviewing their accounts for unauthorized transactions and notifying it immediately if they discover any unauthorized purchases. Plaintiffs and the other Class members now face a greater risk of identity theft.

V. CLASS ALLEGATIONS

104. Pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure Plaintiffs bring claims on behalf of themselves and as a class action on behalf of a "Class" defined as:

> All persons who used Payoneer's payment platform within the statute of limitation through the date of any class certification order in this action and whose data was misused by cybercriminals and incurred reasonable expenses or time spent in mitigation of the consequences of the breach of their Accounts.

Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff. Excluded from the Class are any identified users of Payoneer, who committed fraud in accessing other Accounts without their knowledge and authorization.

105. Pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring claims on behalf of themselves and as a class action, on behalf of a "Subclass" defined as:

> All Payoneer customers who (1) notified Defendant that transactions on their Account were unauthorized; and (2) were improperly denied reimbursement of their Funds within the statute of limitations through the date of any class certification order in this action.

Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff. Excluded from the Class are any identified users of Payoneer, who committed fraud in accessing other Accounts without their knowledge and authorization.

106. Pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring a claim on behalf of themselves and as a class action, on behalf of a "EFTA Class"

defined as:

> All persons in the Class who (1) were denied a return of funds from an unauthorized transaction within the statute of limitations through the date of any class certification order in this action and (2) whose denial was with regard to a disputed charge (or charges) totaling more than $50.

Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff. Excluded from the Class are any identified users of Payoneer, who committed fraud in accessing other Accounts without their knowledge and authorization.

107. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

108. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, Class members number in the tens if not hundreds of thousands.

109. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Payoneer misrepresented the security measures and risks to its customers of third parties accessing their Accounts and stealing their funds;

b. Whether Payoneer failed to use reasonable care and commercially reasonable methods to secure and safeguard Plaintiffs' and Class members' Accounts and Private Information;

c. Whether Payoneer properly implemented its purported security measures to protect Plaintiffs' and Class members' Funds and Private Information from theft and unauthorized capture, dissemination, and misuse;

d. Whether Payoneer took reasonable measures to determine the extent of unauthorized access to its customers' Accounts after it first learned of same;

e. Whether Payoneer engaged in unfair, unlawful, or deceptive practices by failing to safeguard the private information and funds of Plaintiffs and Class Members;

f. Whether Payoneer committed consumer fraud;

g. Whether Payoneer violated the EFTA;

h. Whether Payoneer violated the consumer protection statutes invoked herein;

i. Whether Payoneer's conduct constitutes breach of contract;

j. Whether Payoneer's conduct constitutes unjust enrichment w;

k. Whether Payoneer willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and Class members' Accounts and Private Information;

l. Whether Payoneer was negligent in failing to properly secure and protect Plaintiffs' and Class members' Accounts and Private Information;

m. Whether Plaintiffs and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

110. Payoneer engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of herself and other Class members. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

111. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the other Class members because, among other things, all Class members were similarly injured through Payoneer's uniform misconduct described above and were thus all subject to Payoneer's failed security measures to safeguard their Funds and Private Information alleged herein. Further, there are no defenses available to Payoneer that are unique to Plaintiffs.

112. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other Class members they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The Classes' interests will be fairly and adequately protected by Plaintiffs and their counsel.

113. **Insufficiency of Separate Actions—Federal Rule of Civil Procedure 23(b)(1).** Absent a representative class action, members of the Class would continue to suffer the harm described herein, for which they would have no remedy. Even if separate actions could be brought by individual consumers, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated consumers, substantially impeding their ability to protect their interests, while establishing incompatible

standards of conduct for Payoneer. The Class thus satisfies the requirements of Fed. R. Civ. P. 23(b)(1).

114. **Injunctive Relief – Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted or refused to act on grounds that apply generally to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole. Defendant has uniformly failed to implement adequate security measures to protect customer funds and personal information. Defendant's inadequate security measures and responses to unauthorized transactions have affected all members of the Classes similarly, making injunctive relief appropriate for the Classes as a whole.

115. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Payoneer, so it would be impracticable for Class members to individually seek redress for Payoneer's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CLAIMS

COUNT I: VIOLATION OF NEW YORK GENERAL BUSINESS LAW § 349
By Plaintiffs on Behalf of Themselves and the Class and Subclass

116. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein and further allege as follows:

117. Deceptive Acts and Practices: Payoneer engaged in deceptive acts and practices by misrepresenting the security measures of its platform and failing to protect customers' Funds and Personal Information. This was consumer-oriented conduct that impacted consumers at large and was materially misleading.

118. Origin of Deceptive Conduct: The deceptive conduct originated from Payoneer's headquarters in New York, New York. Payoneer's representations about the security and reliability of their services were made and controlled from New York. These misrepresentations were disseminated from New York to customers worldwide, including the Plaintiffs.

119. Specific Deceptive Acts:

a. Payoneer advertised its services as secure and trustworthy, promising customers that their funds and personal information were safe.

b. Payoneer claimed to use advanced security measures, , to protect customer accounts.

c. Payoneer failed to disclose that its security measures were inadequate, leaving customer accounts vulnerable to unauthorized access and theft.

d. Payoneer continued to represent that its platform was secure even after becoming aware of significant security vulnerabilities and breaches.

120. Harm to Plaintiffs and Class Members: As a result of Payoneer's deceptive practices, Plaintiffs and class members suffered significant financial losses. Unauthorized access

to their Accounts led to theft of Funds and their Personal Information, causing direct economic harm and further future harm from the misuse of their Personal Information. Additionally, Plaintiffs and class members incurred expenses and loss of time in attempting to secure their Accounts and recover their stolen Funds.

121. Causation: Plaintiffs relied on Payoneer's representations regarding the security of its platform. They entrusted their funds and personal information to Payoneer based on these assurances. The class members all suffered harm directly caused by Payoneer's assurances.

122. Geographic Nexus: The deceptive conduct had a sufficient nexus to New York. Payoneer's headquarters and primary operations related to the deceptive practices are based in New York. The representations and assurances made to Plaintiffs and class members were controlled and disseminated from New York.

123. Consumer-Oriented Conduct: Payoneer's deceptive acts and practices were directed at consumers, including individuals and small businesses, who used Payoneer's platform for financial transactions. These consumers reasonably expected that their Funds and Personal Information would be protected as advertised.

124. Violation of GBL § 349: Payoneer's actions constitute violations of New York General Business Law § 349, which prohibits deceptive acts and practices in the conduct of any business, trade, or commerce or in the furnishing of any service in New York.

125. WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, request that this Court enter a judgment against Payoneer, Inc. and award the following relief:

A. Actual Damages: An award of actual damages to compensate Plaintiffs and class members for their financial losses and other economic harm resulting from Payoneer's deceptive practices.

B. Treble Damages: Treble damages up to $1,000 for each Plaintiff and class member, pursuant to New York General Business Law § 349(h).

C. Statutory Damages: Statutory damages as authorized by GBL § 349.

D. Attorney's Fees and Costs: An award of reasonable attorney's fees and costs incurred in bringing this action, as provided by GBL § 349(h).

E. Injunctive Relief: Plaintiffs seek an injunction requiring Payoneer to implement adequate security measures to protect customer funds and personal information and to cease making deceptive representations regarding the security of its platform and to provide accurate information to customers about the risks and security measures associated with their Accounts. Specifically, Plaintiffs seek an injunction to require Payoneer:

i. To utilize privacy and theft protection measures consistent with industry standards.

ii. Implement real-time monitoring and alerts for unauthorized access and transactions.

iii. Provide a means for customers to immediately block accounts, limit amounts that may be paid and transactions in the event of suspicious activity.

iv. Ensure prompt and thorough investigation of all customer complaints regarding unauthorized transactions and restoring stolen funds.

F. Other Relief: Any other relief the Court deems just and proper.

COUNT II: VIOLATION OF DELAWARE CONSUMER FRAUD ACT 6 DEL. C. § 2513 ET SEQ.
By Plaintiffs on Behalf of Themselves and the Class and Subclass

126. Plaintiffs incorporate by reference paragraphs 1-115 as if fully set forth herein and further allege as follows:

127. Defendant Payoneer engaged in deceptive acts and practices by misrepresenting the security measures of its platform and failing to protect customers' funds and personal information. These acts include:

- Advertising and promoting their services as secure and reliable.

- Promising advanced security measures to protect customer accounts.

- Failing to disclose known vulnerabilities in its security measures and systems.

- Continuing to claim that their platform was secure even after multiple security breaches.

128. These deceptive acts and practices were consumer-oriented, affecting a large number of consumers, who relied on Payoneer's representations for the safety of their Funds and Personal Information.

129. As a result of Payoneer's deceptive practices, Plaintiffs and class members suffered significant financial losses due to unauthorized access to their Accounts and theft of Funds.

130. Plaintiffs and class members also incurred expenses and lost time in attempting to secure their accounts and recover their stolen funds.

131. Plaintiffs relied on Payoneer's representations regarding the security of its platform, entrusting their Funds and Personal Information to Payoneer based on these assurances.

132. The financial losses and expenses incurred by Plaintiffs and class members were directly caused by Payoneer's deceptive practices and failures.

133. Defendant's actions constitute violations of the Delaware Consumer Fraud Act, 6 Del. C. § 2513 et seq., which prohibits deceptive acts and practices in the conduct of any trade or commerce.

134. WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, request that this Court enter a judgment against Payoneer Inc. and award the following relief:

A. Actual Damages: Compensation for financial losses and other economic harm resulting from Payoneer's deceptive practices.

B. Treble Damages: Treble damages as provided under the Delaware Consumer Fraud Act.

C. Attorney's Fees and Costs: An award of reasonable attorney's fees and costs incurred in bringing this action.

D. Injunctive Relief: An injunction requiring Payoneer to implement adequate security measures to protect customer funds and personal information and to cease making deceptive representations regarding the security of its platform.

E. Other Relief: Any other relief the Court deems just and proper.

COUNT III: VIOLATION OF DELAWARE DECEPTIVE TRADE PRACTICES ACT 6 DEL. C. § 2532
By Plaintiffs on Behalf of Themselves and the Class and Subclass

135. Plaintiffs incorporate by reference paragraphs 1-115 as if fully set forth herein and further allege as follows:

136. Defendant Payoneer engaged in deceptive trade practices as defined by the Delaware Deceptive Trade Practices Act, 6 Del. C. § 2532, including:

- Causing a likelihood of confusion or misunderstanding regarding the security and reliability of its services.

- Misrepresenting the quality and standard of its security measures.

- Engaging in conduct that creates a likelihood of confusion or misunderstanding about the effectiveness and reliability of its security protocols.

137. As a result of Payoneer's deceptive conduct, Plaintiffs and other Payoneer users suffered damage of unauthorized access to their Accounts that allowed cybercriminals to steal their

Funds and Personal Information. They further face the risk of ongoing harm through identity theft and fraud because cybercriminals possess their Personal Information.

138. Plaintiffs seek injunctive relief to prevent Payoneer from continuing its deceptive trade practices, including:

- Implementing real-time monitoring and alerts for unauthorized access and transactions.

- Providing a means for customers to immediately block accounts and transactions in the event of suspicious activity.

- Ensuring prompt and thorough investigation of all customer complaints regarding unauthorized transactions and restoring stolen funds.

139. WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, request that this Court enter a judgment against Payoneer Inc. and award the following relief:

A. Injunctive Relief: An injunction to prevent Payoneer from engaging in further deceptive trade practices.

B. Attorney's Fees and Costs: An award of reasonable attorney's fees and costs incurred in bringing this action.

C. Other Relief: Any other relief the Court deems just and proper.

COUNT IV: VIOLATION OF THE ELECTRONIC FUND TRANSFER ACT (EFTA)
By Plaintiffs on Behalf of Themselves and the EFTA Class

140. Plaintiffs incorporate by reference paragraphs 1-115 as if fully set forth herein and further allege as follows:

141. Electronic Fund Transfer Act: The Electronic Fund Transfer Act, 15 U.S.C. § 1693 et seq. (EFTA), and its implementing Regulation E, 12 C.F.R. § 1005 et seq., establish the rights, liabilities, and responsibilities of participants in electronic fund transfer systems. Plaintiffs and class members are "consumers" as defined by the EFTA.

142. Payoneer is a "financial institution" as defined by the EFTA, and the Accounts held by Plaintiffs and class members are "accounts" as defined by the EFTA. Payoneer holds and manages customer funds and facilitates electronic transfers, aligning with the definitions in the EFTA.

143. Unauthorized Electronic Fund Transfers: Plaintiffs and class members experienced unauthorized electronic fund transfers from their Payoneer Accounts, which were initiated by third parties without their authority.

144. Failure to Investigate and Resolve Unauthorized Transfers: Payoneer failed to properly investigate and resolve the unauthorized electronic fund transfers in a timely manner as required by 15 U.S.C. § 1693f and 12 C.F.R. § 1005.11. Specifically:

a. Payoneer did not conduct a reasonable investigation of the unauthorized transactions reported by Plaintiffs and class members.

b. Payoneer failed to provisionally credit the Accounts of Plaintiffs and class members within ten (10) business days of receiving notice of the unauthorized transfers.

c. Payoneer improperly denied claims for reimbursement of unauthorized transfers, providing only partial refunds or no refunds at all.

145. Notice of Error: Plaintiffs and class members provided timely notice of the unauthorized electronic fund transfers to Payoneer, fulfilling their obligations under 15 U.S.C. § 1693f and 12 C.F.R. § 1005.11.

146. Damages: As a direct and proximate result of Payoneer's violations of the EFTA, Plaintiffs and class members suffered actual damages, including but not limited to the loss of Funds, deprivation of access to their funds, and other consequential damages.

147. Statutory Damages: Plaintiffs and class members are entitled to statutory damages as provided under 15 U.S.C. § 1693m(a), due to Payoneer's failure to comply with the provisions of the EFTA.

148. Attorney's Fees and Costs: Plaintiffs and class members are entitled to recover reasonable attorney's fees and costs incurred in connection with this action, as provided under 15 U.S.C. § 1693m(a)(3).

149. WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, request that this Court enter a judgment against Payoneer and award the following relief:

A. Actual Damages: An award of actual damages to compensate Plaintiffs and class members for their financial losses and other economic harm resulting from Payoneer's violations of the EFTA.

B. Statutory Damages: Statutory damages as authorized by 15 U.S.C. § 1693m(a).

C. Attorney's Fees and Costs: An award of reasonable attorney's fees and costs incurred in bringing this action, as provided by 15 U.S.C. § 1693m(a)(3).

D. Injunctive Relief: An injunction requiring Payoneer to comply with the requirements of the EFTA and to implement procedures to promptly and adequately investigate and resolve unauthorized electronic fund transfers.

E. Other Relief: Any other relief the Court deems just and proper.

COUNT V: NEGLIGENCE
By Plaintiffs on Behalf of Themselves and the Class and Subclass

150. Plaintiffs incorporate by reference paragraphs 1-115 as if fully set forth herein and further allege as follows:

151. Payoneer owes numerous duties to Plaintiffs and the other members of the Class

and Subclass. These duties include:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Funds and Private Information in its possession;

b. to protect Funds and Private Information in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a Hack and to timely act on warnings about them, including promptly notifying Plaintiffs and the other members of the Class and Subclass.

152. Payoneer knew or should have known the risks of collecting and storing Funds and Private Information and the importance of maintaining secure payment systems. Payoneer knew or should have known of the many unauthorized transactions that targeted other payment platforms in the years before the Hack.

153. Payoneer knew or should have known that its payment systems did not adequately safeguard Plaintiffs' and the other Class and Subclass members' Funds and Private Information.

154. Payoneer breached the duties it owes to Plaintiffs and Class and Subclass members in several ways, including:

a. failing to implement adequate security systems, protocols and practices sufficient to protect customer's Funds and Private Information and thereby creating a foreseeable risk of harm;

b. failing to comply with the minimum industry data security standards including during the time of the Hack; and

c. failing to timely and accurately disclose to customers that their Funds and Private

Information had been improperly acquired or accessed.

155. Payoneer was negligent in transmitting Plaintiffs' and the other Class and Subclass members' Funds and Private Information over compromised electronic networks it had control over and should have known were compromised or susceptible to compromise.

156. But for Payoneer's wrongful and negligent breach of the duties it owed to Plaintiffs and the other Class and Subclass members, their Funds and Private Information would not have been compromised.

157. The injury and harm that Plaintiffs and the other Class and Subclass members suffered was the direct and proximate result of Payoneer's negligent conduct.

158. WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, request that this Court enter a judgment against Payoneer and award the following relief:

A. Actual Damages: An award of actual damages to compensate Plaintiffs and class members for their financial losses and other economic harm resulting from Payoneer's negligence.

B. Attorney's Fees and Costs: An award of reasonable attorney's fees and costs incurred in bringing this action.

C. Injunctive Relief: An injunction requiring Payoneer to implement procedures to promptly and adequately investigate and resolve unauthorized electronic fund transfers.

D. Other Relief: Any other relief the Court deems just and proper.

COUNT VI: BREACH OF CONTRACT
By Plaintiffs on Behalf of Themselves and the Class and Subclass

159. Plaintiffs incorporate by reference paragraphs 1-115 as if fully set forth herein and further allege as follows:

160. In signing up to use Payoneer, Plaintiffs and the other members of the Class and Subclass entered a contract with Payoneer, whereby Payoneer became obligated to reasonably safeguard Plaintiffs' and the other Class and Subclass members' Funds and Private Information.

161. Under the contract, Payoneer was obligated to not only safeguard the Funds and Private Information, but also to provide Plaintiffs and the other Class and Subclass members with prompt, truthful, and adequate notice of any security breach or unauthorized access of Funds or Private Information.

162. Payoneer breached the contract with Plaintiffs and the other members of the Class and Subclass by failing to take reasonable measures to safeguard their Funds and Private Information.

163. Payoneer also breached its contract with Plaintiffs and the other Class and Subclass members by failing to provide prompt, truthful, and adequate notice of the Hack and unauthorized access of their Funds and Private Information by hackers.163. Plaintiffs and the other Class and Subclass members suffered and will continue to suffer damages including, but not limited to: (i) unauthorized access to their Funds and failure to return them; (ii) improper disclosure of their Private Information; (ii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Hack; (iii) the value of their time spent mitigating the increased risk of identity theft and/or identity fraud; (iv) the increased risk of identity theft; and (v) deprivation of the value of their Funds and Private Information, which is likely to be sold to cybercriminals on the dark web. At the very least, Plaintiffs and the other Class and Subclass members are entitled to nominal damages.

164. WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, request that this Court enter a judgment against Payoneer and award the following relief:

A. Actual Damages: An award of actual damages to compensate Plaintiffs and class members for their financial losses and other economic harm resulting from Payoneer's breach of contract.

B. Attorney's Fees and Costs: An award of reasonable attorney's fees and costs incurred in bringing this action.

C. Injunctive Relief: An injunction requiring Payoneer to implement procedures to promptly and adequately investigate and resolve unauthorized electronic fund transfers.

D. Other Relief: Any other relief the Court deems just and proper.

COUNT VII: UNJUST ENRICHMENT
By Plaintiffs on Behalf of Themselves and the Class and Subclass

165. Plaintiffs incorporate by reference paragraphs 1-115 as if fully set forth herein and further allege as follows:

166. Plaintiffs and the other Class and Subclass members conferred a monetary benefit on Payoneer. Specifically, Plaintiffs and the other Class and Subclass members pay for Payoneer services and entrust it with their Funds and Personal Information. In exchange, Plaintiffs and the other Class and Subclass members were entitled to have Payoneer protect their Funds and Private Information with adequate security.

167. Payoneer knew that Plaintiffs and the other Class and Subclass members conferred a benefit on Payoneer. Payoneer profited from Plaintiffs' and the other Class and Subclass members' use of its services through their payment of fees and entrusting their Funds and Private Information to Payoneer.

168. Payoneer failed to secure Plaintiffs' and the other Class and Subclass members' Funds and Private Information and therefore did not provide full compensation for the benefit the

Plaintiffs and the other Class and Subclass members provided. Payoneer inequitably acquired its customers' fees, Funds and Private Information because it failed to disclose its inadequate security practices.

169. If Plaintiffs and the other Class and Subclass members knew that Payoneer would not secure their Funds and Private Information using adequate security, they would not have signed up to use Payoneer services.

170. Plaintiffs and the other Class and Subclass members have no adequate remedy at law.

171. Under the circumstances, it would be unjust for Payoneer to be permitted to retain any of the benefits that Plaintiffs and the other Class and Subclass members conferred on it.

172. Payoneer should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiffs and the other Class and Subclass members proceeds that it unjustly received from them. In the alternative, Payoneer should be compelled to refund the amounts that Plaintiffs and the other Class and Subclass members overpaid.

COUNT VIII: NEGLIGENCE PER SE
By Plaintiffs on Behalf of Themselves and the Class and Subclass

173. Plaintiffs incorporate by reference paragraphs 1-115 as if fully set forth herein and further allege as follows:

174. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Payoneer, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Payoneer's duty in this regard.

175. Payoneer violated Section 5 of the FTC Act by failing to use reasonable measures to protect Funds and Private Information and not complying with applicable industry standards, as described herein. Payoneer's conduct was particularly unreasonable given the nature and amount of Funds and Private Information it stores obtained and stored, and the foreseeable consequences of a Hack involving a payment platform, including, specifically, the damages that would result to Plaintiffs and Class and the Subclass members.

176. Payoneer's violation of Section 5 of the FTC Act constitutes negligence *per se*.

177. Plaintiffs and Class and Subclass members are within the class of persons that the FTC Act was intended to protect.

178. The harm that occurred as a result of the Hack is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, due to their failure to employ reasonable security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class and Subclass.

179. As a direct and proximate result of Payoneer's negligence *per se*, Plaintiffs and the Class and Subclass suffer injuries, including: loss of their Funds accessed through unauthorized transactions; additional false or fraudulent charges stemming from the Hack; damages from lost time and effort to mitigate the actual and potential impact of the Hack on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

180. WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, request that this Court enter a judgment against Payoneer and award the following relief:

A. Actual Damages: An award of actual damages to compensate Plaintiffs and class members for their financial losses and other economic harm resulting from Payoneer's negligence per se.

B. Attorney's Fees and Costs: An award of reasonable attorney's fees and costs incurred in bringing this action.

C. Injunctive Relief: An injunction requiring Payoneer to implement procedures to promptly and adequately investigate and resolve unauthorized electronic fund transfers.

D. Other Relief: Any other relief the Court deems just and proper.

VII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of all claims so triable.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Classes proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Payoneer, as follows:

A. Declaring that this action is a proper class action, certifying the Classes as requested herein, designating Plaintiffs as Class Representatives, and appointing Class Counsel as requested in Plaintiffs' motion for class certification;

B. Ordering Payoneer to pay actual and statutory damages to Plaintiffs and the other members of the Classes;

C. Ordering Payoneer to pay punitive damages, as allowable by law, to Plaintiffs and the other members of the Classes;

D. Ordering Payoneer to pay attorneys' fees and litigation costs to Plaintiffs;

E. Ordering Payoneer to pay equitable relief, in the form of disgorgement and restitution, and injunctive relief;

F. Ordering Payoneer to pay both pre- and post-judgment interest on any amounts awarded; and

G. Ordering such other and further relief as may be just and proper.

Dated: July 16, 2024

Respectfully submitted,

ANDERSEN SLEATER SIANNI LLC

/s/ Jessica J. Sleater
Jessica J. Sleater
Andersen Sleater Sianni LLC
64 Laurel Mountain Ct.
Carmel, NY 10512
Tel: (314) 775-4414
Jessica@andersensleater.com

Ralph N. Sianni
2 Mill Road
Suite 202
Wilmington, DE 19806
Tel: (302) 595-9102
rsianni@andersensleater.com

VARNELL & WARWICK, P.A.

/s/ Janet R. Varnell
Janet R. Varnell, FBN: 0071072
Brian W. Warwick, FBN: 0605573
400 N. Ashley Drive, Suite 1900
Tampa, FL 33602
Telephone: (352) 753-8600
Facsimile: (352) 504-3301
jvarnell@vandwlaw.com
bwarwick@vandwlaw.com
*pro hac vice pending

LAW OFFICE OF ARIEL BERSCHADSKY

/s/ Ariel Berschadsky
Ariel Berschadsky
30 Wall Street, 8th Floor
New York, NY 11201
Tel: (212) 372-3322
ab@berschadsky.com